PATENT ABSTRACTS OF JAPAN

(11)Publication numb r : 2000-148276
(43)Dat of publication of application : 26.05.2000

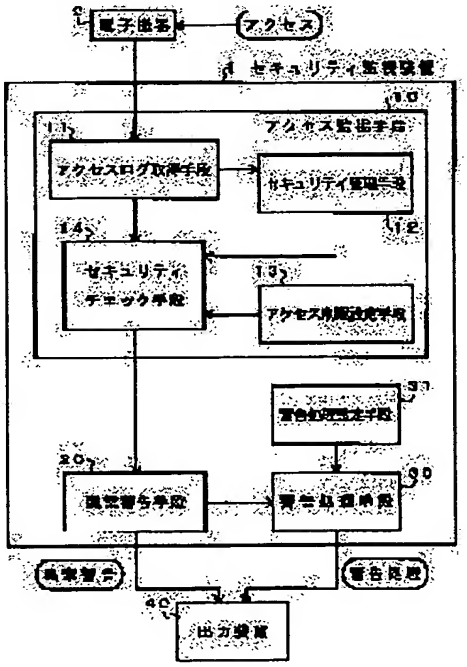
(51)Int.Cl. G06F 1/00
G06F 15/00

(21)Application number : 10-314134
(22)Date of filing : 05.11.1998

(71)Applicant : FUJITSU LTD
(72)Inventor : SEKIGUCHI MINORU

(54) DEVICE AND METHOD FOR MONITORING SECURITY AND SECURITHY MONITORING PROGRAM RECORDING MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To enable the security monitor device, which monitors access on equipment having an external access means, to maintain and manage the security closely even if user authentication information leaks.
SOLUTION: An access monitor means 10 stores an access log as security management information when access is gained, detects th difference from the obtained security management information from the current access and the past access log to decide whether or not the access is different from normal access, and generates an alarm by an abnormality alarm means 20 if the access is different from the normal access. Further, an alarm processing means 30 once informed of the alarm from the abnormality alarm means 20 performs a specific alarm process set by an alarm process setting m ans 31.



LEGAL STATUS

[Date of request for examination] 27.08.2003
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted r gistration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rej ction]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2000－148276
（Ｐ２０００－１４８２７６Ａ）
(43)公開日　平成12年５月26日(2000.5.26)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
G06F 1/00	370	G06F 1/00	370	E 5B085
15/00	330	15/00	330	A

審査請求　未請求　請求項の数11　ＯＬ　（全15頁）

(21)出願番号　特願平10－314134

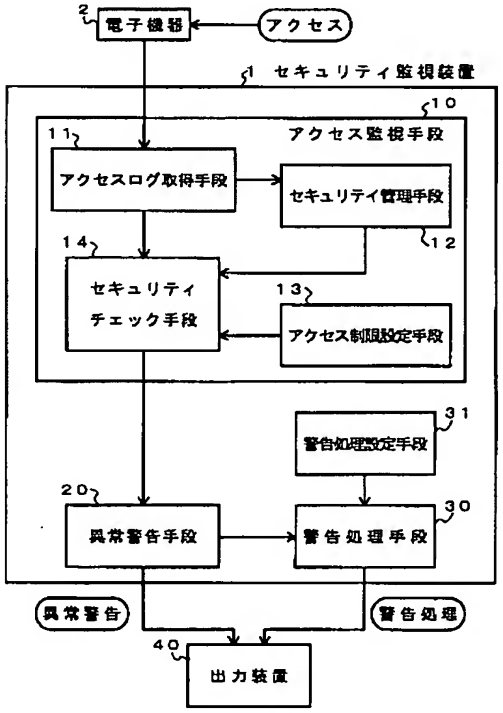
(22)出願日　平成10年11月５日(1998.11.5)

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(72)発明者　関口　実
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(74)代理人　100087848
弁理士　小笠原　吉義　（外２名）

Ｆターム(参考)　5B085 AC14 AE03 AE06

(54)【発明の名称】セキュリティ監視装置，セキュリティ監視方法およびセキュリティ監視用プログラム記録媒体

(57)【要約】
【課題】　外部からのアクセス手段を有する機器においてアクセスを監視するセキュリティ監視装置に関し，ユーザ認証情報が漏洩したような場合でも，セキュリティの維持管理を強固に行うことができるようにする。
【解決手段】　アクセス監視手段１０は，アクセスがあった時にアクセスログをセキュリティ管理情報として蓄積し，現在のアクセスと過去のアクセスログから得られたセキュリティ管理情報との差異を検出することにより，通常のアクセスとは異なるアクセスであるかどうかを判別し，通常のアクセスと異なるときは異常警告手段２０により警告を発する。さらに，警告処理手段３０は，異常警告手段２０からの警告通知を受けて，警告処理設定手段３１によって設定された所定の警告処理を行う。



1

【特許請求の範囲】

【請求項１】　電子機器に対する外部からのアクセスを監視するセキュリティ監視装置において，アクセス時のアクセス状況に関するアクセスログを取得するアクセスログ取得手段と，取得したアクセスログを，セキュリティ管理情報として蓄積し管理するセキュリティ管理手段と，前記セキュリティ管理情報に基づいて現在のアクセスが通常のアクセスと異なるアクセスであるかどうかをチェックするセキュリティチェック手段と，現在のアクセスが通常のアクセスと異なるアクセスである場合に警告を発する異常警告手段とを備えることを特徴とするセキュリティ監視装置。

【請求項２】　請求項１記載のセキュリティ監視装置において，前記セキュリティチェック手段は，現在のアクセスのアクセスログと前記セキュリティ管理情報とを比較し，現在のアクセス状況が過去のアクセス状況の範囲に含まれない場合に，通常のアクセスと異なるアクセスであると判断することを特徴とするセキュリティ監視装置。

【請求項３】　請求項１または請求項２記載のセキュリティ監視装置において，異常として検出すべきアクセス状況に関する条件を定義するアクセス制限を設定できるアクセス制限設定手段を備え，前記セキュリティチェック手段は，前記アクセス制限設定手段により設定されたアクセス制限に基づいて，警告を発すべき異常アクセスであるかどうかを判断することを特徴とするセキュリティ監視装置。

【請求項４】　請求項３記載のセキュリティ監視装置において，前記アクセス制限設定手段は，セキュリティレベルに応じた複数の設定情報を保持し，前記セキュリティチェック手段は，アクセス状況に応じて変更されるセキュリティレベルに応じて，使用する設定情報を使い分けることを特徴とするセキュリティ監視装置。

【請求項５】　請求項１記載のセキュリティ監視装置において，ユーザからのアクセスに対して前記セキュリティチェック手段により異常アクセスが検出されたとき，そのユーザに第２のパスワードを要求し，それが正当と認められる場合にアクセスを許可する警告処理手段を備えることを特徴とするセキュリティ監視装置。

【請求項６】　請求項１記載のセキュリティ監視装置において，前記セキュリティチェック手段により異常アクセスが検出されたとき，そのアクセスをどのように禁止または許可するかを設定できる警告処理設定手段と，前記警告処理設定手段による設定情報に基づいて警告処理を実行する警告処理手段とを備えることを特徴とするセキュリティ監視装置。

【請求項７】　請求項１記載のセキュリティ監視装置において，前記セキュリティ管理手段が管理するセキュリティ管理情報は，ユーザのアクセス時刻に関して統計的に処理したアクセス時間帯の情報を含み，前記セキュリティチェック手段は，前記セキュリティ管理情報におけるアクセス時間帯以外のアクセスに対して異常アクセスと判断することを特徴とするセキュリティ監視装置。

2

【請求項８】　請求項１記載のセキュリティ監視装置において，前記アクセスは，キーボード，マウス等のコンピュータ等への入力手段を介するもの，機器へのログイン，ファイルへのアクセス，機器を操作するための実行コマンド，またはネットワーク経由のアクセスであることを特徴とするセキュリティ監視装置。

【請求項９】　監視用入力機器からの入力を監視するセキュリティ監視装置において，前記監視用入力機器により画像または音声情報を入力する画像・音声入力部と，入力した画像・音声のログ情報を，セキュリティ管理情報として蓄積し管理する画像・音声ログ管理手段と，前記セキュリティ管理情報に基づいて，入力された画像または音声情報が通常と異なる画像または音声情報であるかどうかをチェックするセキュリティチェック手段と，入力された画像または音声情報が通常と異なる場合に警告を発する異常警告手段とを備えることを特徴とするセキュリティ監視装置。

【請求項１０】　電子機器に対する外部からのアクセスを監視するセキュリティ監視方法において，アクセス時のアクセス状況に関するアクセスログを取得する過程と，取得したアクセスログを，セキュリティ管理情報として蓄積し管理する過程と，前記セキュリティ管理情報に基づいて現在のアクセスが通常のアクセスと異なるアクセスであるかどうかをチェックする過程と，現在のアクセスが通常のアクセスと異なるアクセスである場合に警告を発する過程とを有することを特徴とするセキュリティ監視方法。

【請求項１１】　電子機器に対する外部からのアクセスを監視するセキュリティ監視方法をコンピュータによって実現するためのプログラムを記録した記録媒体であって，アクセス時のアクセス状況に関するアクセスログを取得する処理と，取得したアクセスログを，セキュリティ管理情報として蓄積し管理する処理と，前記セキュリティ管理情報に基づいて現在のアクセスが通常のアクセスと異なるアクセスであるかどうかをチェックする処理と，現在のアクセスが通常のアクセスと異なるアクセスである場合に警告を発する処理とを，コンピュータに実行させるプログラムを記録したことを特徴とするセキュリティ監視用プログラム記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は，電子機器のセキュリティ保護の技術に係り，詳しくは，ユーザに負担をかけることなく複雑な電子機器のセキュリティの維持管理を実現する電子機器のセキュリティ監視装置，セキュリティ監視方法およびセキュリティ監視用プログラム記録媒体に関する。

【０００２】
【従来の技術】従来，コンピュータ等の電子機器では，アクセス管理等のセキュリティを維持，管理するために，ユーザＩＤとパスワードによるユーザ管理方式，暗号化によるデータ漏洩防止方式，アクセス制御方式，認証方式など，さまざまなセキュリティのための監視方式が開発されている。
【０００３】このようなセキュリティ監視方式は，主にあらかじめ設定したユーザ等の管理情報（ユーザＩＤやパスワード等）とユーザが何らかの機器操作をする時点で要求される管理情報とを照合し，それらが規定通りに一致するかまたは許容範囲内にあると認められる場合に，ユーザの要求を実行するものである。すなわち，ユーザの認証に基づくセキュリティ管理を基本としていた。
【０００４】
【発明が解決しようとする課題】しかし，このようなユーザＩＤやパスワード，アクセス制限などのユーザの認証に基づくセキュリティ管理方式では，不正アクセスがあったかどうかを調べるために，常時，そのアクセスログを正規ユーザ自身や管理者が調べ，自分もしくは正規ユーザがアクセスしたものかどうかを確認するなどのアクセスログの管理が必要であった。これには，簡単なユーザＩＤとパスワードではすぐに不正にアクセスされるという根本的欠点があり，ユーザがアクセスログをいちいちチェックしておく必要があって大変面倒であるなどの問題点があった。また，ログ管理を多かれ少なかれ人手に頼っているため，アクセスの正当性の確認に時間がかかり，結果として，不正が発覚するまでに時間がかかっていた。
【０００５】また，ユーザ認証情報が漏洩した場合には，不正アクセスがあったかどうかを確認するのに多くの手間と時間がかかるため，不正の発見が遅れるといった問題があった。
【０００６】以上のような理由で，ユーザの認証に基づくセキュリティ管理方式は，基本的に認証情報の漏洩に対して，まったくセキュリティ機能が働かないか，またはセキュリティの維持管理にも多くの労力がかかるという欠点があった。
【０００７】また，ネットワーク経由のアクセスであって，メールサーバ等のメール受信プロトコルのような基本的にはユーザが介在しない半自動的アクセスは，通常特定ユーザ名を利用して，ある種の特定実行権限をもってほぼ自動的にアクセスしてくるので，セキュリティには十分注意する必要がある。しかし，不正ユーザやウイルス等は，このようなセキュリティの弱点を利用してアクセスしてくる場合が多く，ユーザ認証に基づくセキュリティ監視では，このようなアクセスに対しても基本的に無力である。
【０００８】一方，暗号化によるセキュリティ方式では，ネットワークを利用したデータ転送時や不正ユーザによるアクセス時に重要な情報が解読されないというようなメリットはあるものの，不正ログインや不正アクセスに対しては無力である。
【０００９】本発明の目的は，このようなユーザの認証に基づくセキュリティの維持，管理方式によらず，ユーザやネットワークからのアクセス状況を監視し，通常とは異なるアクセスを検出して警告を発することによって，もしユーザの認証情報が漏洩した場合でも，より強固なセキュリティの維持管理を行うセキュリティ監視方式を提供することにある。
【００１０】
【課題を解決するための手段】本発明は，監視対象の電子機器に対する外部からのアクセスを監視し，過去のアクセス状況に関するアクセスログ（セキュリティ管理情報）を参照することにより，新たなアクセスが過去のアクセスログから異常と思われる場合に，何らかの警報を発する機構を持つことをもっとも主要な特徴とする。
【００１１】すなわち，外部からのアクセス手段を有する電子機器において，アクセス時のアクセス環境や時刻などのアクセス状況を取得し，蓄積しておき，そのアクセス状況が所定の基準に該当する場合に，管理者またはユーザに対して何らかの警告を発する。電子機器へのアクセス方法の代表的なものとして，例えばネットワーク，キーボード，マウス等のコンピュータ等への入力手段がある。電子機器へのアクセス内容の代表的なものとしては，例えば機器へのログイン，ファイルへのアクセス，機器を操作するための実行コマンド，ネットワーク経由のアクセスがある。
【００１２】また，アクセス状況の基準を，アクセス頻度，アクセス内容（書き込み，読み込み，実行など）に応じて，設定する手段を設けることもできる。例えば過去のアクセスログから得られるセキュリティ管理情報によって，最初のアクセスからある一定回数または一定期間は警告を発するが，何度も同じアクセスを繰り返すと，警告を発しないようにすることができる。
【００１３】さらに，あるユーザからのアクセスがあった際に，セキュリティ監視による警告が発せられた後，アクセスをどのように禁止または許可するかを設定する機構を加えることができる。また，パスワードによるセキュリティ管理機構を持つ装置において，あるユーザからのアクセスがあった際に，上記セキュリティ管理情報に基づく警告を発した後，再度，ユーザに対して第２のパスワードを要求し，入力されたパスワードが正当と認められる場合にアクセスを許可する機構を設けることもできる。
【００１４】セキュリティ管理情報における時間帯を，ユーザのアクセス時刻に関して正規分布等を用いて統計的に処理し，アクセス時刻の分散値を基準にその警告する範囲を決定することも可能である。

【００１５】セキュリティレベルを管理するため，複数のセキュリティ管理情報やアクセス制限情報に関する設定ファイルを利用し，時間経過やアクセス回数などのユーザのアクセス時間経過に応じて，使用する設定ファイルを変更し，セキュリティレベルを変更管理する機構を設けることもできる。これにより，例えば新規ユーザ登録時などに，初期設定したアクセス状況を利用して，新規ユーザに対しては通常ユーザとは異なるセキュリティチェックを適用することができる。

【００１６】以上の各処理機構をコンピュータによって実現するためのプログラムは，コンピュータが読み取り可能な可搬媒体メモリ，半導体メモリ，ハードディスクなどの適当な記録媒体に格納することができる。

【００１７】

【発明の実施の形態】図１は，本発明の概要を説明するための図である。本発明に係るセキュリティ監視装置１では，コンピュータ等の電子機器２において，アクセス時のアクセス環境や時刻などのアクセス状況を常に監視するアクセス監視手段１０と，通常アクセスとは異なるようなアクセスがあった場合に警告を発し，何らかの異常アクセスが発生したことを管理者または特定ユーザに通知する異常警告手段２０とを備える。さらに，異常警告手段２０による異常警告に伴い，アクセスを一時的に禁止するなどの警告処理設定手段３１によって設定された所定の警告処理を実施する警告処理手段３０を備える。なお，図１では，電子機器２とセキュリティ監視装置１とを区別して表しているが，セキュリティ監視装置１は，電子機器２の中に組み込まれて電子機器２と一体化したものであってもよい。

【００１８】具体的には，電子機器２に対してアクセスがあった場合に，アクセス監視手段１０は，アクセスログ取得手段１１によりアクセスログを取得し，そのアクセスログを，セキュリティ管理手段１２により統計処理して，セキュリティ管理情報として保存する。また，セキュリティチェック手段１４により，アクセスログ取得手段１１が取得したアクセスログと，過去のアクセスログから得られたセキュリティ管理情報とを比較することによって，今回のアクセス状況と，過去のアクセス状況との差異を検出し，通常とは異なる状況でされたアクセスを異常アクセスと判断し，異常警告手段２０により管理者や特定のユーザに警告を発する。

【００１９】また，セキュリティチェック手段１４によるアクセスログとセキュリティ管理情報との比較において，アクセス制限設定手段１３により事前に設定されたアクセス制限を考慮に入れることもできる。今回のアクセスのアクセスログが，設定されたアクセス制限に該当するものである場合には，異常警告手段２０により管理者や特定のユーザに警告を発する。さらに，警告処理設定手段３１による設定に基づいて，警告処理手段３０は，ユーザＩＤのロック，アクセス禁止，第２パスワードの要求等の警告処理を行う。

【００２０】したがって，ユーザ認証情報の漏洩があり，不正ユーザが，正規のユーザとは異なる方法や環境でアクセスを行った場合でも，通常のアクセスと異なる状況でされたアクセス（異常アクセス）として認識し，警告を発することができる。さらに，予め設定しておいた警告処理を直ちに行うことができ，より強固なセキュリティを実現することができる。

【００２１】以下，本発明の実施の形態について図面を参照してさらに詳しく説明する。本発明では，原理的には，ユーザの認証情報といったものは不要である。しかし，現在の電子機器ではこのようなセキュリティ管理方法は一般的であり，本発明においても，ユーザの認証情報を利用することによって，より強固なセキュリティレベルを確保できる。したがって，以下に説明する本発明の実施の形態では，従来のユーザ認証に基づくセキュリティ方式に加えて，本発明の方式を用いたものについて説明する。

【００２２】〔第１の実施の形態〕まず，第１の実施の形態について説明する。ここでは，コンピュータ等の電子機器に対するアクセスを監視する場合を例にする。

【００２３】図２は，本発明の第１の実施の形態についての構成例を示すブロック図である。アクセス監視部１１０は，監視対象の電子機器に対するアクセスを監視し，ユーザから何らかのアクセスがあると，そのアクセスが通常とは異なるアクセスであるかどうかを検出する。通常どおりのアクセスであれば，そのまま何もせずにアクセス監視が続けられる。しかし，このアクセスが何らかの異常アクセスであると判断されると，異常警告部１２０に，そのアクセスが異常であることが報告され，異常警告部１２０は，異常であることを出力装置１４０を介して特定ユーザまたは管理者に警告する。

【００２４】このアクセス監視部１１０は，電子機器へのアクセスログ２０１を収集するアクセスログ取得部１１１，アクセスログ取得部１１１が収集したアクセスログを統計処理し，セキュリティ管理情報２０３として管理するセキュリティ管理部１１２，異常として検出する条件を定義するアクセス制限情報２０４の設定を行うアクセス制限設定部１１３，アクセスが異常アクセスであるかどうかをチェックするセキュリティチェック部１１４から構成される。セキュリティチェック部１１４は，アクセスログ２０１とセキュリティ管理情報２０３との比較により異常アクセスを検出するログ比較部１１５，アクセスが設定されたアクセス制限情報２０４の制限にかかるかどうかを比較する制限比較部１１６からなる。

【００２５】アクセスログ取得部１１１は，アクセスログ２０１を取得する。機器へのアクセス方法として，他の機器によるネットワークからのアクセス，キーボード，マウス等のコンピュータ等へのさまざまな入力手段からのアクセスがあり，それらのアクセスログを取得す

る。

【００２６】図３は，取得されたアクセスログの例を示す図であり，コンピュータへのアクセスについてのアクセスログ２０１を示す。アクセスログ２０１として，ユーザ名，パスワード，アクセス日時，アクセスしたファイルのファイル名，実行したコマンドのコマンド名等の情報が収集され記憶される。アクセスログ２０１は，セキュリティ管理部１１２に送られる。

【００２７】セキュリティ管理部１１２は，アクセスログ取得部１１１が取得したアクセスログ２０１を統計処理し，ユーザごとに，アクセス頻度，アクセス日時の時間帯（何時から何時にアクセスしているか，何曜日にアクセスしているかなど），過去にアクセスしたファイル名とそのアクセス頻度，アクセスした時間帯，実行したコマンドのコマンド名とその実行頻度，実行した時間帯などのセキュリティ管理情報２０３に変換して保管する。アクセスログ２０１は，ファイルごとまたはコンピュータごとに統計処理し，セキュリティ管理情報２０３として保管してもよい。

【００２８】図４は，ユーザに関するセキュリティ管理情報の例を示し，図５はコンピュータに関するセキュリティ管理情報の例を示す。図４のユーザに関するセキュリティ管理情報２０３は，ユーザごとに保管される情報であり，ユーザのパスワード，アクセス回数，初回および前回のアクセス日時およびアクセス時間帯，アクセスしたファイルごとの初回および前回のアクセス日時，アクセス頻度，アクセス時間帯，実行コマンドごとの初回および前回の実行日時，実行頻度，実行時間帯，アクセスするコンピュータ等の情報である。

【００２９】図５のコンピュータに関するセキュリティ管理情報２０３は，コンピュータごとに保管される情報であり，登録ユーザ名，アクセスしたファイルごとの初回および前回のアクセス日時，アクセス頻度，アクセス時間帯，実行コマンドごとの初回および前回の実行日時，実行頻度，実行時間帯，アクセスするコンピュータまたはアクセスされたコンピュータごとの初回および前回のアクセス日時，アクセス頻度，アクセス時間帯等の情報である。

【００３０】図４または図５に示すセキュリティ管理情報２０３の情報のうち，時間帯の情報に関して，ユーザまたは他のコンピュータがアクセスする時間は，きちんと何時から何時までとは決まっていないし，アクセスを繰り返すうちに徐々にずれてくる場合もある。

【００３１】そのため，セキュリティ管理部１１２では，統計的な処理により，アクセス時間帯の範囲を決定する方法を用いて管理する。例えば，あるユーザのアクセスする時刻を，図６に示すような正規分布と仮定すると，その分布は平均ｍと分散ｓで表される。したがって，ユーザアクセスを正常と判断する時間帯をｍ±３ｓのように分散の±３ｓの範囲とすれば，あるユーザが過去にアクセスしてきた時間帯のうち約９９．７％の時間帯についてアクセスを無条件で許可するように設定することができる。このようなアクセスに対する統計情報を，過去全部というように区間を区切らずに計算するか，または必要に応じて例えば過去１ケ月とか１年とかいう区間を区切るかして計算し，それをもとにアクセスを許可する時間帯を設定する。このような方法を用いれば，ユーザのアクセス時間帯が初期設定によらず，ユーザの利用状況によって自動的に変化するので，都合がよい。

【００３２】ログ比較部１１５は，アクセスログ取得部１１１が取得した今回のアクセスのアクセスログ２０１と過去に取得したログ情報から得られるセキュリティ管理情報２０３のアクセス状況を比較する。比較は，セキュリティ管理情報２０３として保管してある状況のすべてまたは一部について行う。比較する内容は，あらかじめユーザが設定するか，または管理者が決めてもよい。また，所望するセキュリティのレベルに応じて変更してもよい。

【００３３】ここで，ユーザｕｓｅｒＡについて，アクセス日時，アクセスファイル，実行コマンドの三種についてセキュリティを管理するものとすれば，それぞれの項目について，今回のアクセスがそのセキュリティ管理情報２０３の範囲内のアクセスであったかどうかについてログの比較を行い，そのセキュリティ管理情報２０３の範囲内であれば，通常アクセスであるものとして，次の制限比較部１１６の処理に移る。

【００３４】例えば，アクセスしたファイルの比較では，過去にアクセスしたことのないファイルにアクセスした場合には，セキュリティ管理情報２０３の範囲外として，警告を発するように異常警告部１２０に指令を出す。また，実行コマンドの比較では，過去に実行したことのあるコマンドかどうかを比較し，セキュリティ管理情報２０３に記録のない実行コマンドであれば，警告を発するよう異常警告部１２０に指令を出す。

【００３５】例えば，あるユーザｕｓｅｒＡのアクセスが，図３に示すようなアクセスログ２０１であり，一方，このユーザｕｓｅｒＡに対して図４に示すようなセキュリティ管理情報２０３が保存されている場合，ログ比較の結果，このアクセスの時間は１８：３０：３４であるから，セキュリティ管理情報２０３のアクセス時間帯１０：００：００－１９：００：００の範囲内となり，ここでは異常なアクセスではないと判断され，さらに制限比較部１１６により，アクセス制限に該当するかどうかをチェックする処理に進む。

【００３６】一方，ユーザｕｓｅｒＡのアクセス時間が２１：００：００である場合には，セキュリティ管理情報２０３の範囲外となるので，ログ比較部１１５から警告を発することを指示する指令を異常警告部１２０に出す。

【００３７】制限比較部１１６は，今回のアクセスログ２０１を，アクセス制限設定部１１３によって事前に設定したアクセス制限情報２０４の該当箇所と比較する。比較の結果，アクセスログ２０１がアクセス制限情報２０４で設定された範囲外すなわちアクセス可であるならば，警告は発せずに，また次のアクセス待ちとなる。一方，アクセスログ２０１がアクセス制限情報２０４の範囲内，すなわちアクセス制限にかかる場合には，異常警告部１２０に対し，このアクセスがアクセス制限にかかった旨の警告指令を出す。

【００３８】アクセス制限設定部１１３は，制限比較部１１６で用いるための各ファイルや実行コマンドについてのアクセス制限情報２０４を設定する。図７は，設定されたアクセス制限情報の例を示す。

【００３９】アクセス制限情報２０４は，ファイルへのアクセスまたはコマンドの実行を制限する場合のアクセス頻度，アクセス時間の範囲に関する情報である。例えば，ユーザごとに，アクセスファイル設定として，特定のファイルに対し，「アクセス頻度３以下」，「アクセス時間帯９：００：００－１８：００：００以外」というような設定がなされる。また，コマンド実行設定として，特定のコマンドに対し，「実行頻度－１以下」，「実行時間帯０：００：００－０：００：００以外」などのような設定がなされる。

【００４０】アクセス制限情報2-0-4へのアクセスファイル設定では，ユーザごとに個々のファイルのアクセス可否を設定することにより，ユーザのアクセス管理を行うことができる。例えば管理者のみがアクセスできる管理者ファイルに対して，一般ユーザからのアクセスを制限したい場合，一般ユーザのアクセス制限情報２０４として，その管理者ファイルへのアクセス制限時間を０：００：００－０：００：００以外のように全時間帯にしておけば，その管理者ファイルへのアクセスを常に許可しないようにすることができる。

【００４１】同様に，アクセス制限情報２０４は，例えばコンピュータのシステム管理用コマンドを一般ユーザに実行させないようにするときにも利用することができる。このような管理用コマンドに対して，アクセス制限情報２０４のアクセス頻度をアクセス頻度を無限大（図７に示すアクセス制限情報２０４の例ではマイナスの値で代用している）まで許可しないように設定しておけば，一般ユーザからの管理用コマンドの実行が制限されることになる。

【００４２】ＵＮＩＸ系ＯＳなどではファイル属性を変えることによってアクセス管理を行えるが，本方式では，どのユーザがいつどこからアクセスしたか，そのアクセスは通常アクセスなのかそれとも通常とは異なるアクセスなのかというような状況に基づいて，より詳細なファイルアクセスの監視が可能となる。

【００４３】異常警告部１２０は，アクセス監視部１１０から異常であることの報告を受ける異常警告受信部１２１とその異常警告を受けて実際にどのような警告を発するかを決定し警告を発する警告発信部１２２からなる。

【００４４】異常警告受信部１２１がアクセス監視部１１０から異常発生の通知を受けとると，異常の内容を調べて，どこの誰に警告を発するかを決定し，警告発信部１２２は，出力装置１４０を介して警告を発する。警告は，ログ情報として特定のファイルに保存されるようにしてもよいし，システム管理者へメールで送るようにしたり，ディスプレイ等の表示装置に表示するようにしてもよい。

【００４５】例えばユーザｕｓｅｒＡに対して図４に示すようなセキュリティ管理情報２０３が保管されている状態で，図３のアクセスログ２０１に示すようなアクセスがあったとする。ユーザｕｓｅｒＡに対するアクセス制限情報２０４としては，図７に示すようなアクセス制限が設定されているとする。ユーザｕｓｅｒＡのファイルｆｉｌｅ１．ｔｘｔへのアクセスは，セキュリティ管理情報２０３でのアクセス頻度が２２であるから，アクセス頻度「３以下」の範囲外であるが，アクセス日時が１８：３０：３４であり，制限時間帯「９：００：００－１８：００：００以外」の範囲内となる。したがって，異常なアクセスとして警告が発せられることになる。また，コマンドｅｘｅｃ．ｅｘｅの実行は，セキュリティ管理情報２０３では実行頻度が６２となっているから，実行頻度「３以下」の範囲外であるが，実行日時が１８：３２：２０であり，制限時間帯「９：００：００－１８：００：００以外」の範囲内となり，同様に警告が発せられる。

【００４６】警告の具体例は，以下のとおりである。ユーザｕｓｅｒＡのアクセス時間が午後９時であった場合には，ユーザｕｓｅｒＡの通常のアクセス時間帯と異なるので，アクセス監視部１１０から通知を受けた異常警告部１２０の警告発信部１２２から，「警告：ｕｓｅｒＡは異常な時間午後９時にログインしました。」というような警告が，基本的には管理者に対して発せられる。また，ユーザｕｓｅｒＡのアクセスが，過去にアクセスしたことのないファイルに対するものである場合には，「警告：ｕｓｅｒＡは過去にアクセスしたことのないファイルＦにアクセスしました。」というような警告が発せられる。

【００４７】ユーザＩＤとパスワード等によるユーザ認証を行うシステムにおいて，このような状況は，ユーザｕｓｅｒＡのＩＤやパスワード等の認証情報が盗まれたような場合に起こると考えられる。例えば，ユーザｕｓｅｒＡの通常のアクセス時間帯である午前１０時から午後７時の間以外の時間にアクセスがあった場合には，通常のアクセス時間帯と違うので，別のユーザがユーザｕｓｅｒＡのＩＤとパスワードを用いてアクセスしている

可能性があり，通常の時間帯でない時間にアクセスがあった旨の警告が発せられる。

【００４８】また，コンピュータがネットワーク接続されているような状況においては，あるコンピュータから別のコンピュータに相互ログインすることが多い。このような場合，ユーザが通常どのコンピュータからアクセスしているかをあらかじめ取得しておけば，通常のコンピュータとは別のコンピュータからアクセスしていることを検出した場合に，別のユーザの不正なアクセスである可能性があることから，通常とは違ったコンピュータからアクセスされた旨の警告を発することが可能である。したがって，本方式によれば，ユーザのＩＤやパスワードが盗まれた場合でも，本来の正規ユーザが使用しないアクセス状況であれば異常なアクセスとして警告が発せられるので，より強固なセキュリティが確保できる。

【００４９】図２に示すセキュリティチェック部１１４においては，説明を簡単にするために，ログ比較部１１５による異常アクセスの検出と，制限比較部１１６によるアクセス制限情報２０４に基づく異常アクセスの検出とが，独立に行われるものとして説明した。しかし，セキュリティチェック部１１４における異常アクセスの検出を，ログ比較部１１５による検出と制限比較部１１６による検出とを関連させた形態で行うようにしてもよい。例えば，所定の設定ファイルに従って，双方で異常と検出した場合にのみ，警告を発するような実施も可能である。また，セキュリティチェック部１１４を，ログ比較部１１５または制限比較部１１６の一方だけで構成することも可能である。ログ比較部１１５による比較条件を，アクセス制限情報２０４または他の設定情報に基づいて決定するような実施も可能である。

【００５０】以上で説明した方式では，基本的に過去にアクセスしたことがないユーザに関しては，セキュリティ管理情報２０３に過去のアクセス履歴の蓄積がないことから，常に警告を発することになる。すなわち，新規ユーザは，すべてのアクセスに関して警告を発せられることになり，管理上煩わしいことにもなる。そこで，新規ユーザが警告なしに利用できるように，初期設定として，通常考えられるファイルへのアクセスやアクセス時間帯などを設定した新規ユーザに対するアクセス制限情報を別に用意しておく。こうすれば，このような煩わしい状況を回避することができる。

【００５１】また，正規ユーザが正規の方法でアクセスする場合でも，最初は警告を発するが，何度もそのアクセスを繰り返せば，アクセス頻度が上がるので，指定回数以上のアクセス頻度になったら警告しないようにアクセス制限情報を別に設けておけば，所定アクセス回数後のアクセスは，正常なアクセスとして警告を発しなくすることもできる。

【００５２】図８は，新規ユーザに対するアクセス制限情報の例を示す図である。新規ユーザに対するアクセス制限情報２０５は，新規ユーザや特定のセキュリティレベルのユーザに対して適用する。新規ユーザに対するアクセス制限情報２０５が適用されるユーザについては，所定期間経過後または所定アクセス回数後，例えば１週間とか３回目のアクセスとかいう時点でセキュリティレベルを通常ユーザ用のセキュリティレベルに変更する。これにより，以後，図８に示す新規ユーザ用のアクセス制限情報２０５に代わり，図７に示すような通常ユーザに対するアクセス制限情報２０４が適用される。

【００５３】新規ユーザに対するセキュリティレベルと，通常ユーザに対するセキュリティレベルの違いによって，アクセス制限情報を使い分ける例を説明したが，同様にさまざまなセキュリティレベルに対応させたアクセス制限情報を用意することにより，セキュリティレベルを細かく区分して，セキュリティレベルに応じたアクセス監視を実現することもできる。

【００５４】また，電子機器へのアクセスとしては，ユーザからのアクセスだけでなく，ネットワーク内の他の機器からの半自動的アクセスもあり得る。例えば，メールサーバなどがそうである。メールは，メールサーバやメールを受信したコンピュータ内のある種のプログラムを起動することができるので，セキュリティの確保が難しい。本方式では，このような基本的にユーザが介在しないコンピュータ同士のアクセスについてもセキュリティの監視が可能である。

【００５５】図９は，メールサーバのネットワークを経由するアクセスから得られるアクセスログの例を示す。セキュリティ管理部１１２は，図９に示すアクセスログ２０６を，図１０に示すようなセキュリティ管理情報２０７に変換して記憶しておく。

【００５６】この場合のログ比較処理は，例えば次のように行われる。ログ比較部１１５は，図９のアクセスログ２０６と図１０のセキュリティ管理情報２０７とを比較し，そのアクセスログ２０６のアクセスが，セキュリティ管理情報２０７に記録されている既存の送信者からのメールであれば，警告なしに受信する。しかし，セキュリティ管理情報２０７に記録されていない送信者からのメールである場合には，異常警告部１２０に異常を通知し，異常警告部１２０は，例えば次のような警告を発する。

【００５７】「警告：未知のユーザからメールが送られてきました。」このような警告を，管理者またはメールの宛先ユーザに対して発することにより，管理者または宛先ユーザは，そのメールを読まずに削除するなり，ウイルスに感染しても構わないコンピュータで読むなりして，任意に処置することができるようになるので，セキュリティの適切な維持・管理が可能となる。

【００５８】図１１に，第１の実施の形態による処理の流れの概要を示す。アクセスログ取得部１１１によりア

クセスログ２０１を取得し，セキュリティ管理情報２０３に変換してセキュリティ管理部１１２に記録する（ステップＳ１）。次に，ログ比較部１１５により，アクセスログ２０１とセキュリティ管理情報２０３とを比較し（ステップＳ２），アクセスログ２０１の内容がセキュリティ管理情報２０３の範囲内であるかどうかにより，通常アクセスかどうかを判断する（ステップＳ３）。通常アクセスでない場合には，ステップＳ６へ進み，異常警告部１２０によって異常警告を発する。通常アクセスである場合には，さらに，制限比較部１１６によりアクセスログ２０１とアクセス制限情報２０４とを比較し（ステップＳ４），アクセスログ２０１がアクセス制限の範囲内であるかどうかを判断する（ステップＳ５）。アクセスログ２０１がアクセス制限情報２０４に基づくアクセス制限の範囲内であれば，異常警告部１２０により異常警告を発し（ステップＳ６），アクセスログ２０１がアクセス制限の範囲外であれば，異常の警告を発することなく，次のアクセスを待つ。

【００５９】図1.2は，本発明を適用するもっとも代表的なハードウェアの構成例を示す。この例では，コンピュータ３００は，監視対象の電子機器とセキュリティ監視装置１００とを兼ねる。コンピュータ３００において，ネットワーク3-0.4からのアクセスやコンピュータ３００本体へのキーボードやマウスなどの入力装置３０１からのアクセスが監視され，警告はディスプレイ３０２に表示される。アクセスログやセキュリティ管理情報はハードディスク等の記憶装置３０３に記憶され，比較が必要になった時点で読み出される。また，アクセスが行われるたびにセキュリティ管理情報が更新され，記憶装置３０３に記録される。

【００６０】〔第２の実施の形態〕本方式では，通常でないアクセスと判断した場合には警告を発するが，そのアクセスが正当ユーザからのアクセスであると確認できた場合には，アクセスを許可したほうがよい。また，システムの運用上，警告を発した後にアクセスを許可するのか禁止するのかといった選択ができるほうが望ましい。そこで，第２の実施の形態では，このような場合のために，警告処理の手順をいくつか決めておき，それを選択することができるようになっている。

【００６１】図１３は，本発明の第２の実施の形態についての構成例を示すブロック図である。図１３に示すセキュリティ監視装置４００は，図２に示すセキュリティ監視装置１００と同様の手段を備え，さらに警告処理設定部４１０と警告処理部４２０とを備える。なお，警告処理設定部４１０と警告処理部４２０以外の図１３に示す各手段は，図２に示す同じ番号が付されている手段に対応している。ただし，異常警告部１２０における警告発信部１２２は，出力装置１４０に警告を出力する代わりに，警告処理部４２０に対して警告を通知する。

【００６２】警告処理設定部４１０は，警告を発した後に行う警告処理を設定する手段であり，警告処理部４２０は，異常警告部１２０からの警告の通知を受けて警告処理設定部４１０で設定された情報に従って警告処理を行う手段である。

【００６３】警告処理設定部４１０により，予め設定される警告処理設定の例を，図１４に示す。また，図１５は，各警告処理設定に対応したユーザに対する警告の例，図１６は，各警告処理設定に対応した管理者に対する警告の例を示す。

【００６４】図１４に示す（１）の警告処理設定が行われた場合，警告処理部４２０によって警告が発せられた後，ユーザのアクセスは禁止され，ユーザはロックアウトされる。このとき，ユーザに対して，図１５（１）の「このアクセスは禁止されています。あなたのユーザＩＤはロックされました。再度アクセスするには管理者に連絡してください。」というメッセージが出力される。また，管理者に対しては，図１６（１）の「禁止されたアクセスがありました。ユーザｘｘｘｘｘはロックアウトされました。」というメッセージが出力される。

【００６５】また，図１４に示す（２）の警告処理設定が行われた場合，警告処理部４２０によって警告が発せられた後，ユーザのアクセスは禁止される。このとき，ユーザに対しては，図１５（２）のメッセージが出力され，管理者に対しては，図１６（２）のメッセージが出力される。

【００６６】図１４に示す（３）の警告処理設定が行われた場合，警告処理部４２０によって警告が発せられた後，ユーザのアクセスは管理者の許可が出るまで禁止される。ユーザはそれまで待機する。このとき，ユーザに対しては，図１５（３）のメッセージが出力され，管理者に対しては，図１６（３）のメッセージが出力される。

【００６７】図１４に示す（４）の警告処理設定が行われた場合，警告処理部４２０によって警告が発せられた後，ユーザは第２のパスワードが求められ，それが正当と認められる場合に限り，アクセスが許可される。このとき，ユーザに対しては，図１５（４）のメッセージが出力され，管理者に対しては，図１６（４）のメッセージが出力される。

【００６８】図１４に示す（５）の警告処理設定が行われた場合，警告処理部４２０によって警告が発せられるが，アクセスは許可される。このとき，ユーザに対しては，図１５（５）のメッセージが出力され，管理者に対しては，図１６（５）のメッセージが出力される。

【００６９】図１４に示す（６）の警告処理設定が行われた場合，警告処理部４２０による警告は行われず，通常通りアクセスが続行される。これは“セキュリティなし”の状態と同じであり，ユーザに対す警告メッセージも管理者に対する警告メッセージも出力されない。

【００７０】なお，以上の各警告処理設定に応じた警告

メッセージは，管理者だけに出力して，ユーザ対しては何も出さないようにすることも可能である。図１７に，第２の実施の形態による処理の流れの概要を示す。アクセスログ取得部１１１によりアクセスログ２０１を取得し，セキュリティ管理情報２０３に変換してセキュリティ管理部１１２に記録する（ステップＳ２１）。次に，ログ比較部１１５により，アクセスログ２０１とセキュリティ管理情報２０３とを比較し（ステップＳ２２），アクセスログ２０１の内容がセキュリティ管理情報２０３の範囲内であるかどうかにより，通常アクセスかどうかを判断する（ステップＳ２３）。通常アクセスでない場合には，ステップＳ２６へ進み，異常警告部１２０を介して警告処理部４２０による警告処理を行う。通常アクセスである場合には，さらに，制限比較部１１６によりアクセスログ２０１とアクセス制限情報２０４とを比較し（ステップＳ２４），アクセスログ２０１がアクセス制限の範囲内であるかどうかを判断する（ステップＳ２５）。アクセスログ２０１がアクセス制限情報２０４に基づくアクセス制限の範囲内であれば，ステップＳ２６へ進む。アクセスログ２０１がアクセス制限の範囲外であれば，警告処理を行うことなく，次のアクセスを待つ。

【００７１】ステップＳ２６では，警告処理設定部４１０により事前に設定された警告処理設定に従って，図１５および図16に示すようなメッセージを出力し，図１４に示す警告処理を実行する。

【００７２】〔第3の実施の形態〕第１および第２の実施の形態では，コンピュータへのアクセスの例について説明したが，本方式は，基本的に住居侵入監視，交通監視などの監視を必要とする機器のすべてに応用できる。

【００７３】図１８は，本発明の第３の実施の形態についての構成例を示すブロック図である。セキュリティ監視装置５００は，カメラ監視部５１０，異常警告部５２０，監視カメラ等５３０，表示装置５４０を備える。

【００７４】監視カメラ等５３０は，前述した実施の形態におけるコンピュータの入力手段に相当し，カメラ監視部５１０は，図１に示すアクセス監視手段１０に，異常警告部５２０は異常警告手段２０に，表示装置５４０は出力装置４０に，それぞれ相当する。

【００７５】図１９は，図１８に示す装置を住居侵入監視装置として用いる場合の例を示す。住居侵入監視に関しては，家人の帰宅時間，人数，できれば顔画像などの情報を取得しておき，通常とは異なる時間帯や人が来訪した際に警告を発する。

【００７６】具体的には，家人の帰宅時間，人数，できれば顔画像などの画像情報を監視カメラ等５３０から画像・音声入力部５１１によって取得し，画像・音声ログ管理部５１２に記憶する。さらに，画像・音声比較部５１５により，画像・音声ログ管理部５１２に記憶したこれまでの来訪者等の情報と比較し，通常とは異なる来訪であると判断した場合には，異常警告部５２０により，表示装置５４０に警告メッセージを表示し，またはブザー等を用いて警告する。さらに，制限比較部５１６により，予め設定したアクセス制限情報をもとに，禁止されている来訪者または来訪時間等の来訪であるかを調べて警告を発することもできる。なお，画像を入力する例を説明したが，マイクロホンから入力した音声情報をセキュリティチェックに用いることもできる。

【００７７】図２０は，図１８に示す装置を交通監視装置として用いる場合の例を示す。交通監視では，例えば交差点などのある地点を通る車の情報，ナンバー，車種，運転手などを取得し，指定された車以外の車が通行した際に警告を発する。

【００７８】具体的には，ある地点の通過車の情報，ナンバー，車種，運転手などを監視カメラ等５３０から画像・音声入力部５１１により取得し，画像・音声ログ管理部５１２に記憶する。さらに，画像・音声比較部５１５により，画像・音声ログ管理部５１２に記憶したこれまでの通過車等の情報と比較し，通常とは異なる通過車であると判断した場合には，異常警告部５２０により，表示装置５４０に警告メッセージを表示し，またはブザー等を用いて警告する。さらに，制限比較部５１６により，予め設定したアクセス制限情報をもとに，通過が禁止されている車または運転者等であるかを調べて警告を発することもできる。

【００７９】図２１は，第３の実施の形態による処理の流れの概要を示す。監視カメラ等５３０から画像・音声情報を入力し，画像・音声ログ管理部５１２に記憶する（ステップＳ３１），画像・音声比較部５１５は，入力した画像・音声情報と画像・音声ログ管理部５１２が記憶する画像・音声ログ管理情報とを比較する（ステップＳ３２）。画像・音声ログ管理情報の中に，入力した画像・音声情報と一致するものがあるかどうかを判断し（ステップＳ３３），一致するものがなければ，異常警告部５２０により警告を発する（ステップＳ３６）。画像・音声ログ管理情報に一致するものがある場合には，さらに，制限比較部５１６によりアクセス制限情報と比較し（ステップＳ３４），画像・音声がアクセス制限情報の範囲内であるかどうかを判断する（ステップＳ３５）。画像・音声情報がアクセス制限情報の範囲内であれば，異常警告部５２０により警告を発する（ステップＳ３６）。

【００８０】以上のように，本方式により，

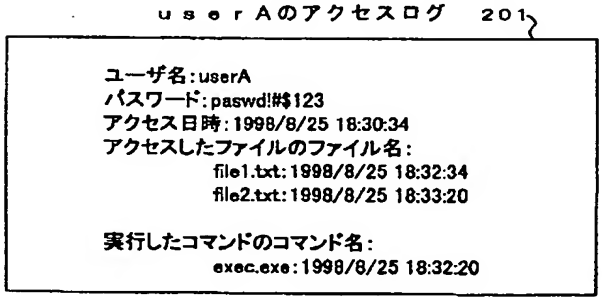
１）アクセス内容に応じたセキュリティ管理情報を保存でき，

２）ログ比較処理で用いる基準を，アクセス頻度，アクセス内容（書き込み，読み込み，実行など）に応じて任意に設定でき，

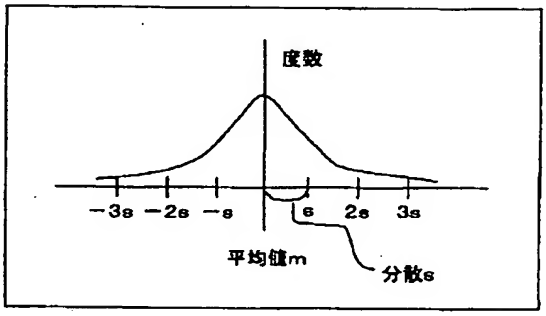
３）アクセス制限情報のアクセス指定期間を無限期間に設定することなどにより，アクセス禁止を設定すること

ができ，
４）セキュリティレベルを管理するため，複数のセキュリティ管理情報ファイルを設けて，時間経過やアクセス回数などのユーザのアクセス時間経過に応じて使用するセキュリティ管理情報ファイルを変更し，セキュリティレベルを変更管理することができ，
５）警告が発せられた後，アクセスをどのように許可するか等の警告処理を設定することができるようになる。
【００８１】したがって，より強固かつ適切なセキュリティ管理を行うことができるようになる。
【００８２】
【発明の効果】以上説明したとおり，本発明によれば，ユーザの認証に基づくセキュリティの維持，管理方式によらず，ユーザやネットワークからのアクセス状況を監視し，通常の状況と異なる状況のアクセスを検出することによって，もしユーザの認証情報が漏洩したような場合であっても不正と考えられるアクセスを検出することができ，強固なセキュリティの維持管理を行うことが可能になる。
【図面の簡単な説明】
【図１】本発明の概要を説明するための図である。
【図２】本発明の第１の実施の形態についての構成例を示すブロック図である。
【図３】アクセスログの例を示す図である。
【図４】ユーザに関するセキュリティ管理情報の例を示す図である。
【図５】コンピュータに関ずるセキュリティ管理情報の例を示す図である。
【図６】あるユーザのアクセス時刻の分布の例を示す図である。
【図７】アクセス制限情報の例を示す図である。
【図８】新規ユーザに対するアクセス制限情報の例を示す図である。
【図９】ネットワーク経由のアクセスから得られるアクセスログの例を示す図である。
【図１０】ネットワーク経由のアクセスから得られるアクセスログのセキュリティ管理情報の例を示す図である。
【図１１】第１の実施の形態による処理の流れの概要を示す図である。
【図１２】第１の実施の形態において本発明を実現するハードウェアの構成例を示す図である。
【図１３】本発明の第２の実施の形態についての構成例を示すブロック図である。
【図１４】警告処理設定の例を示す図である。
【図１５】警告処理設定に応じたユーザに対する警告の例を示す図である。
【図１６】警告処理設定に応じた管理者に対する警告の例を示す図である。
【図１７】第２の実施の形態による処理の流れの概要を示す図である。
【図１８】本発明の第３の実施の形態についての構成例を示すブロック図である。
【図１９】図１８に示すセキュリティ監視装置を住居侵入監視装置として用いる場合の例を示す図である。
【図２０】図１８に示すセキュリティ監視装置を交通監視装置として用いる場合の例を示す図である。
【図２１】第３の実施の形態による処理の流れの概要を示す図である。
【符号の説明】
１　セキュリティ監視装置
２　電子機器
１０　アクセス監視手段
１１　アクセスログ取得手段
１２　セキュリティ管理手段
１３　アクセス制限設定手段
１４　セキュリティチェック手段
２０　異常警告手段
３０　警告処理手段
３１　警告処理設定手段
４０　出力装置

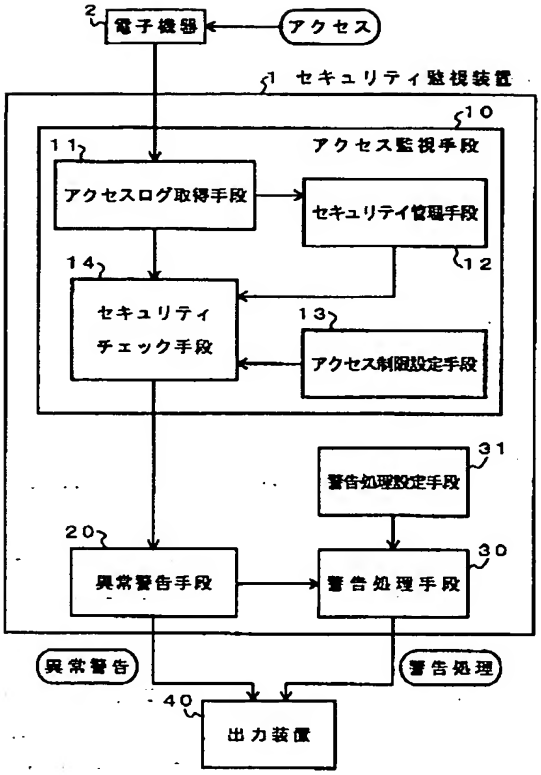
【図３】



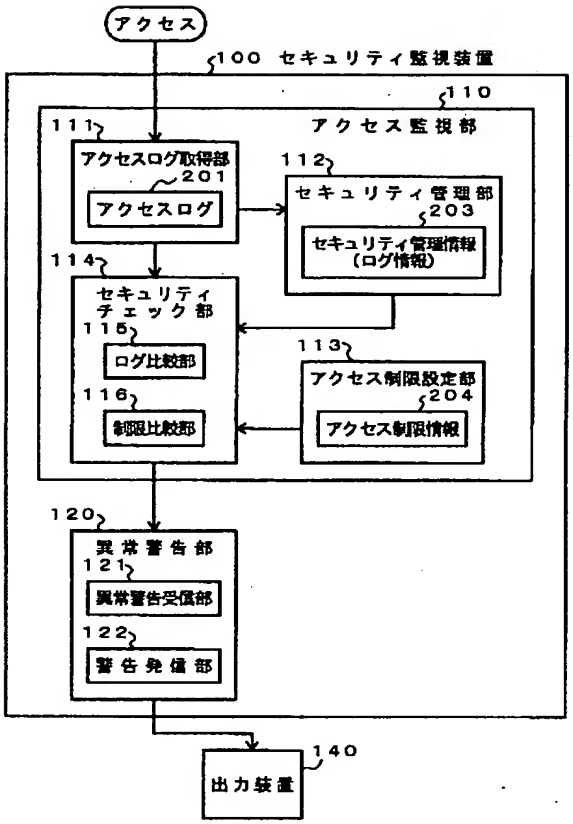
【図６】



【図１】



【図２】



【図４】

セキュリティ管理情報　203

ユーザ名：userA
パスワード：paswd!#$123
アクセス回数：123
アクセス日時：初回：1998/4/25 10:30:34、前回：1998/8/24 10:32:34、時間帯：10:00 :00- 19:00:00
アクセスしたファイル：
　　file1.txt：初回：1997/8/25 12:32:34、前回：1998/8/25 17:30:34、頻度：22、時間帯：12:00:00 - 17:30:34
　　file2.txt：初回：1997/8/30 10:32:34、前回：1998/8/25 17:32:34、頻度：12、時間帯：10:00:00 - 17:32:34
　　exeo.exe：初回：1997/8/30 10:32:34、前回：1998/8/25 18:32:20、頻度：62、時間帯：10:00:00 - 19:30:34
　　・・・
実行したコマンド
　　exeo.exe：初回：1997/8/30 10:32:34、前回：1998/8/25 18:32:20、頻度：62、時間帯：10:00:00 - 19:30:34
　　com.exe：初回：1997/8/31 10:32:34、前回：1998/8/25 18:22:20、頻度：105、時間帯：10:00:00 - 19:30:34
　　・・・
アクセスするコンピュータ：
　　comp1, comp2, comp3
・・・

【図５】

セキュリティ管理情報　203

コンピュータ名：compB
登録ユーザ：userA, userB, ...
アクセスファイル：
　file1.txt：初回：1995/8/25 12:32:34、前回：1998/8/25 17:30:34、頻度：222、時間帯：12:00:00 – 17:30:34
　file2.txt：初回：1997/8/30 10:32:34、前回：1998/8/25 17:32:34、頻度：122、時間帯：10:00:00 – 17:32:34
　exec.exe：初回：1996/5/31 10:32:34、前回：1998/8/27 15:22:50、頻度：305、時間帯：10:00:00 – 15:30:34
　・・・
実行コマンド
　exec.exe：初回：1995/8/30 10:32:34、前回：1998/8/25 18:32:20、頻度：642、時間帯：10:00:00 – 19:30:34
　com.exe：初回：1996/5/31 10:32:34、前回：1998/8/27 15:22:50、頻度：305、時間帯：10:00:00 – 15:30:34
　・・・
アクセスするコンピュータ：
　comp1：初回：1995/3/30 15:22:34、前回：1998/8/22 15:32:20、頻度：542、時間帯：15:00:00 – 16:00:00
　comp2：初回：1995/4/3 15:32:23、前回：1998/8/25 18:32:20、頻度：542、時間帯：15:00:00 – 19:00:34
　・・・
アクセスされたコンピュータ：
　comp1：初回：1995/3/30 15:32:34、前回：1998/8/20 15:32:20、頻度：542、時間帯：15:00:00 – 17:00:34
　comp2：初回：1996/5/20 20:32:35、前回：1998/8/25 18:32:20、頻度：344、時間帯：18:00:00 – 22:30:34
　server1：初回：1995/8/20 8:32:54、前回：1998/8/27 8:32:20、頻度：632、時間帯：4:00:00 – 9:00:14
　server2：
・・・

【図７】

アクセス制限情報　204

ユーザ名：userA
アクセスファイル設定：
　file1.txt：頻度3以下、時間帯9:00:00 – 18:00:00以外
　file2.txt：頻度3以下、時間帯9:00:00 – 18:00:00以外
　file3.txt：時間帯0:00:00 – 0:00:00以外
コマンド実行設定：
　exec.exe：頻度3以下、時間帯9:00:00 – 18:00:00以外
　cmd.exe：頻度-1以下、時間帯0:00:00 – 0:00:00以外

【図８】

アクセス制限情報（新規ユーザ用）　205

ユーザ名：new
アクセスファイル設定：
　file1.txt：頻度0以下、時間帯9:00:00 – 18:00:00以外
　file2.txt：頻度0以下、時間帯9:00:00 – 18:00:00以外
　file3.txt：時間帯0:00:00 – 0:00:00以外
コマンド実行設定：
　exec.exe：頻度0以下、時間帯9:00:00 – 18:00:00以外
　cmd.exe：頻度-1以下、時間帯0:00:00 – 0:00:00以外

【図９】

ネットワーク経由のアクセスログ　206

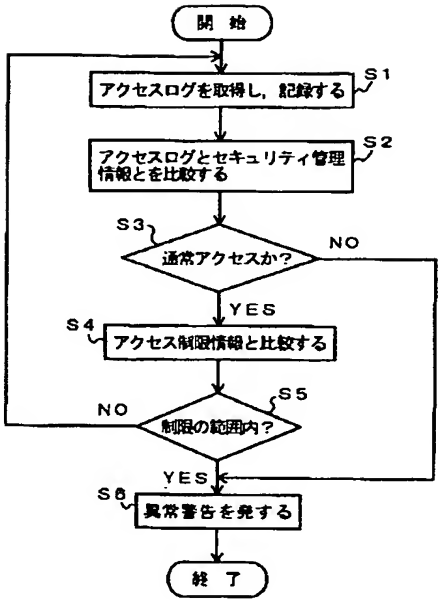
接続してきたコンピュータ名：mailserver1
メールの宛先：userA
メールの送信者：senderX
経由したコンピュータ名：mailserv2, mailserv3
メールの受信日時：1998/3/20 14:22:36
使用プロトコル：smtp

【図１０】

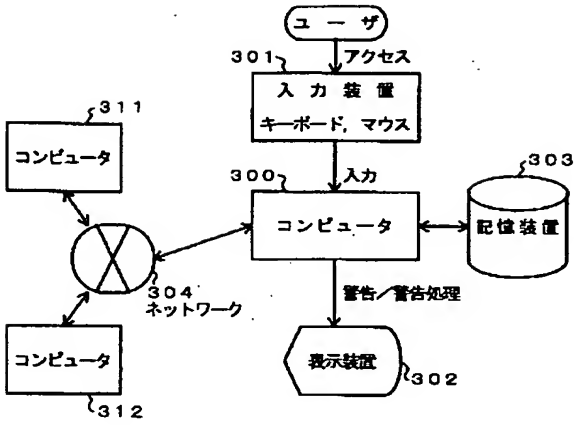
セキュリティ管理情報　207

接続してきたコンピュータ名：mailserver1, mailserv2, ...
メールの宛先：userA, userB, ...
メールの送信者：senderX, senderY, senderZ,....
経由したコンピュータ名：mailserv2, mailserv3
メールの受信日時：1998/3/20 14:22:36
使用プロトコル：smtp, ...

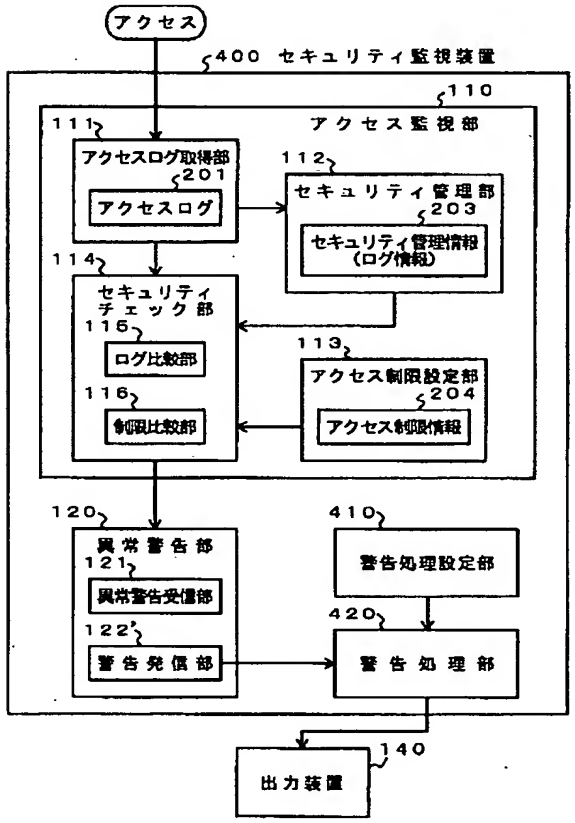
【図１１】



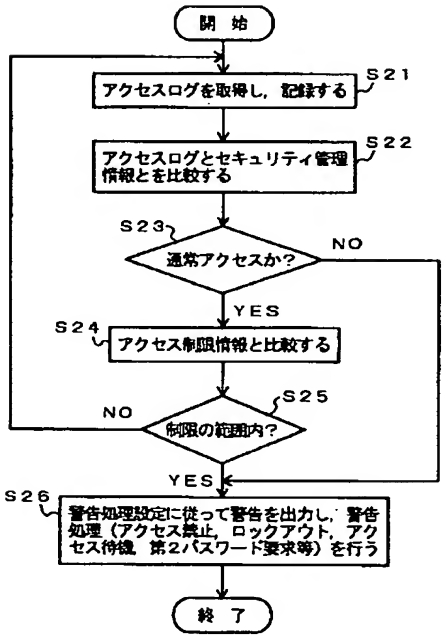
【図１２】



【図１３】



【図１７】



【図１４】

警告処理設定の例

(1)	警告を発し，アクセスを禁止し，ユーザをロックアウトする
(2)	警告を発し，アクセスを禁止する
(3)	警告を発し，管理者が許可するまでアクセスを禁止する。ユーザをそれまで待機させる。
(4)	警告を発し，ユーザに第２のパスワードを求め，それが正当と認められる場合に限り，アクセスを許可する
(5)	警告を発するのみで，アクセスは認める
(6)	通常どおりアクセスを認める

【図１５】

ユーザに対する警告の例

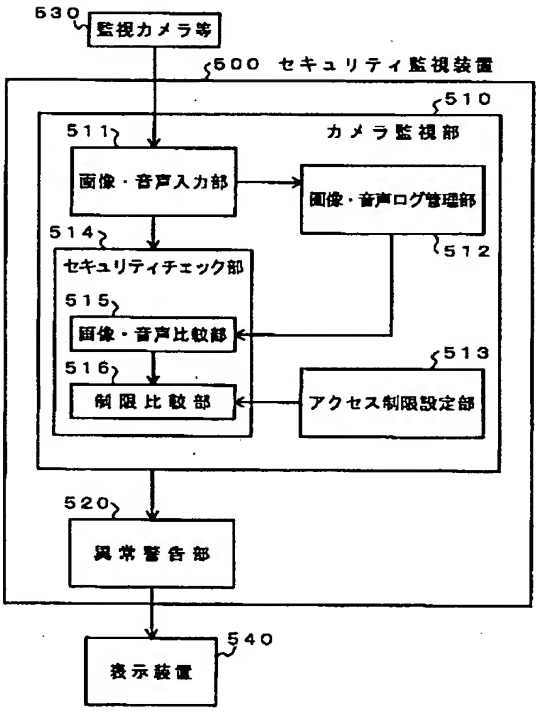
(1)	このアクセスは禁止されています。あなたのユーザＩＤはロックされました。再度アクセスするには管理者に連絡してください。
(2)	このアクセスは禁止されています。
(3)	このアクセスは制限されています。管理者の許可がでるまで，このままお待ちください。
(4)	このアクセスは制限されています。第2パスワードを入力してください。
(5)	このアクセスは通常アクセスではありませんが，アクセスは許可します。
(6)	警告なし

【図１６】

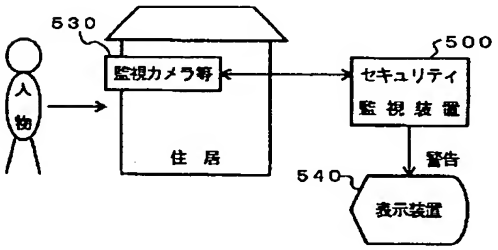
管理者に対する警告の例

(1)	禁止されたアクセスがありました。ユーザ×××××はロックアウトされました。
(2)	禁止されたアクセスがありました。ユーザ：○○○○○
(3)	制限されたアクセスがあります。このアクセスを許可しますか？
(4)	制限されたアクセスがありました。第2パスワードを要求しました
(5)	制限されたアクセスがありました。
(6)	警告なし

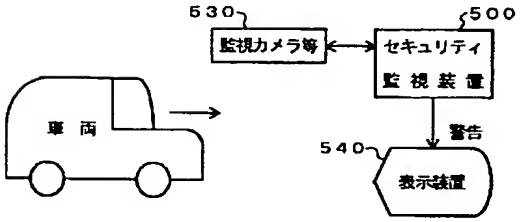
【図１８】



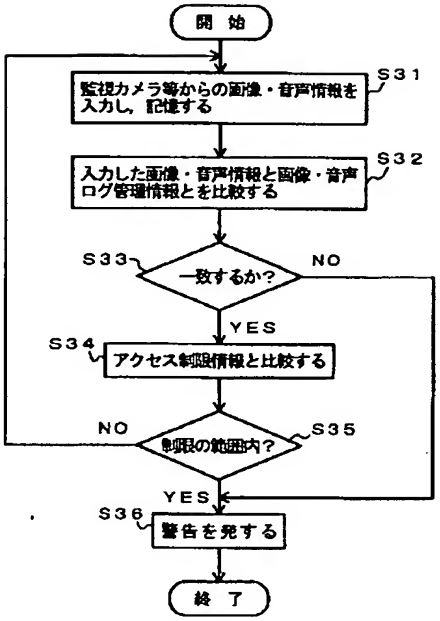
【図１９】



【図２０】



【図２１】


開 始
監視カメラ等からの画像・音声情報を入力し、記憶する
S31
入力した画像・音声情報と画像・音声ログ管理情報とを比較する
S32
S33
一致するか?
NO
YES
S34
アクセス制限情報と比較する
NO
制限の範囲内?
S35
YES
S36
警告を発する
終 了